UNITED STATES DISTRICT COURT

for the

Eastern District of Pennsylvania

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
(a) an Acer laptop; (b) a TCL/Tracphone cellular telephone; and (c) an 'Attache' thumb drive, currently in custody of the FBI, 600 Arch Street, Philadelphia, PA

Case No. 20-247-M

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

(a) Acer laptop; (b) TCL/Tracphone cellular telephone; and (c) 'Attache' thumb drive, further described in Attachment A

located in the Eastern District of Pennsylvania, there is now concealed *(identify the person or describe the property to be seized)*:

Evidence, contraband, fruits and instrumentalities of a crime, further described in Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 USC 2423(a)	transporting a minor in interstate commerce with intent to engage in sexual activity

The application is based on these facts:
See attached Affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

FBI SA Benjamin Jacobs
Printed name and title

Sworn to before me and signed in my presence.

Date: February 19, 2020

Judge's signature

City and state: Philadelphia, PA

Hon. Carol S. Moore Wells, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT

I, Benjamin M. Jacobs, a Special Agent (SA) with the Federal Bureau of Investigation (FBI), Philadelphia Division, being duly sworn, depose and state as follows:

1. I have been employed as a Special Agent of the FBI for nine years. While employed by the FBI, I have investigated federal criminal violations, including the FBI's Innocent Images National Initiative which investigates matters involving the sexual exploitation of children. I have gained experience through training at the FBI Academy, training from the Innocent Images Unit of the FBI, and everyday work related to conducting these types of investigations.

2. As a federal agent, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States.

3. This affidavit is being made in support of an application for a search warrant for: (a) an Acer laptop (Serial Number 05205585825); (b) a TCL/Tracphone (IMEI Number 015283000863287), and (c) an 'Attache' 2 gigabyte thumb drive, currently in the custody of FBI Philadelphia, further described in Attachment A, for evidence, contraband, fruits and instrumentalities of violations of Title 18, United States Code, Section 2423(a), transporting a minor in interstate commerce with the intent to engage in sexual activity, further described in Attachment B.

4. The statements in this Affidavit are based in part on my investigation of this matter and on information provided by other law enforcement officers. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only those facts that I believe are necessary to establish probable cause to believe that evidence of violations of 18 U.S.C. § 2423(a) is contained on: (a) an Acer laptop; (b) a TCL/Tracphone cellular telephone; and (c) an 'Attache' thumb drive, further described in Attachment A.

5. In summary, the following facts establish there is probable cause to believe Michael Swavely (Swavely) did travel with a minor out of the state of Pennsylvania to engage in sexual acts in violation of 18 U.S.C. § 2423(a), and evidence of said violation is contained on: (a) an Acer laptop; (b) a TCL/Tracphone cellular telephone; and (c) an 'Attache' thumb drive, further described in Attachment A.

LEGAL AUTHORITY

6. Title 18 U.S.C. § 2423(a) prohibits a person from knowingly transporting an individual who has not attained the age of 18 years in interstate commerce with the intent that the individual engage in any sexual activity for which any person can be charged with a criminal offense.

BACKGROUND REGARDING COMPUTER/ELECTRONIC DEVICES AND THE INTERNET

7. I have had both training and experience in the investigation of computer related crimes. Based on my training, experience and knowledge, I know the following:

a. Computers and computer technology have revolutionized the way in which photographs are produced, shared, and saved. Photographs formerly were produced using cameras and film (either still photography or movies). The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. As a result, there were definable costs involved with the production of images.

b. The development of computers has added to the methods used by photographers. Computers serve numerous functions in connection with photography. These are production, editing, distribution/sharing, and storage.

c. Cell phones and more advanced devices known as "smart phones" function the same as computers and can run computer software and applications, create and edit files, go on the Internet, chat, text, email, and interact with others on the Internet, and store, send, and receive files, among other functions. Cell phones and smart phones have been used to send, receive, store, and produce images, as well as engage in voice, email, text, and real time chat conversations. Cell phones and smart phones can contain SD cards and/or SIM cards that can store data such as pictures, videos, text messages, contact lists, call logs, internet search history, and other data.

d. GPS, or Global Positioning System, devices can be portable devices used to obtain directions to destinations or show roads and directions in a given area. GPS devices can store the route an individual traveled. GPS devices have been used by individuals to obtain directions when they travel to meet a minor for sexual purposes.

e. Photographs can also be converted into a computer readable format with a device known as a scanner. With the advent of digital cameras, the images can now be transferred directly onto a computer. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection.

f. The computer's ability to store images in digital form makes the computer itself an ideal repository for photographs. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store hundreds of thousands of images at very high resolution.

g. Individuals will also use online resources to retrieve and save photographs, and generate or save business/travel records, including services offered by Internet Portals such as Google, Yahoo!, Hotmail, Sky Drive or One Drive, and Dropbox among others. The online services allow a user to set up an account with a remote computing service that provides e mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer or device, such as a cell phone or "smart phone", with access to the Internet.

h. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an e mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. A forensic examiner often can recover evidence suggesting whether a computer contains peer to peer software, when the computer was sharing files, and some of the files which were uploaded or downloaded. Such information is often maintained indefinitely until overwritten by other data.

FACTS SUPPORTING PROBABLE CAUSE

8. On January 10, 2020, your affiant was contacted by the Berks County District Attorney's Office (BCDA) regarding a complaint received by Fleetwood Police Department (FPD), Fleetwood, Pennsylvania. On December 22, 2019, FPD was contacted by the mother of a 17-year-old boy (Minor 1), date of birth February xx, 2002. Both the mother and son are known to law enforcement, but their names are omitted in this affidavit to protect their identities. The mother advised Minor 1 was sexually assaulted by their neighbor, Michael Swavely, who is a convicted child sexual offender, and currently registered in Pennsylvania's Megan's Law registry. I have independently confirmed Swavely is a Megan's Law registrant.

9. FPD interviewed Minor 1, who stated Swavely was a personal family friend and lived in close proximity to Minor 1 at 121 South Chestnut Street, Fleetwood, Pennsylvania. Minor 1 would visit Swavely in the basement room, which is referred to by Minor 1 and Swavely

as, "the dungeon," almost every day to talk about cars and welding. Minor 1 described the basement room as an approximately 10 feet by 10 feet concrete room. The basement is entered through outside storm doors at the back of the residence, then down a short staircase to a second standard-type door to enter the room. Inside the basement is a work bench with two computers on the bench. The room also contains a small beverage-style refrigerator and various tools and items hanging on the walls. Minor 1 added there is no access to the basement room from the main living area of the house, only through the outside storm doors.

10. Minor 1 stated Swavely began sexually assaulting him in "the dungeon" when he was 12 years old (approximately 2014), and the last sexual contact Swavely had with Minor 1 was January 2019. Swavely would provide Minor 1 with alcohol and cigarettes, and Swavely would fondle Minor 1's penis and scrotum. Swavely later advanced to preforming oral sex on Minor 1. Minor 1 ejaculated during some of these encounters.

11. FPD conducted follow-up interviews with Minor 1's girlfriend, a 16-year-old girl whose identity is known to law enforcement. Minor 1 had confided the same account of the relationship to his girlfriend, and his girlfriend, who also referred to the basement room as "the dungeon," described the room the same way as Minor 1, including the presence of two computers.

12. On December 24, 2019, FPD conducted a non-custodial interview of Swavely in the FPD station where the interview was video and audio recorded. FPD advised Swavely, who was not handcuffed, throughout the interview he was not under arrest and free to leave and stop the interview. During the interview, Swavely admitted to preforming oral sex on Minor 1, and touching his penis. Swavely stated this occurred for approximately two years, from 2015-2017 (which, as your affiant knows, is when Minor 1 would have been between the ages of 13 and 15) but had not occurred for approximately two years. The sexual contact occurred in Swavely's basement room of his residence, which Swavely also referred to as "the dungeon."

13. Swavely said he also sexually assaulted Minor 1 at hotels in the Baltimore, Maryland area. Swavely elaborated he would take Minor 1 on fishing trips to Baltimore, Maryland and Delaware, and he would perform sexual acts on Minor 1 during those trips while staying in hotels in the Baltimore, Maryland and Crisfield, Maryland areas. FPD asked Swavely if he maintained any images from those trips, and Swavely stated he had a few images on his cellular telephone. FPD asked to see the images, and Swavely voluntarily showed FPD two pictures of Minor 1 during some of those trips, which were on Swavely's cellular telephone. At the conclusion of the interview, FPD seized Swavely's cellular telephone and obtained a Pennsylvania State search warrant for the contents of the telephone. After reviewing the extraction report from the search warrant, internal data from those images of Minor 1 showed they were taken in 2015 and 2017, and they were of Minor 1 fishing. FPD asked Swavely if he performed any sexual acts with Minor 1 during those trips memorialized in the two photographs, and Swavely stated he did. Swavely then provided a written statement to FPD confirming the sexual relationship with Minor 1.

14. Further forensic review of Swavely's cellular telephone information showed the phone connected to wireless internet (wifi) service at the following hotels on the following dates:

a. Econolodge on May 12, 2017, July 12-15, 2017, December 29-31, 2017 [Minor 1 was age 15], and February 18, 2018 [Minor 1 was age 16];
b. Comfort Inn on July 13-15, 2017 [Minor 1 was age 15];
c. Days Inn on August 19, 2017 and August 21, 2017 [Minor 1 was age 15];
d. LaQuinta Hotel on July 2, 2018 [Minor 1 was age 16];
e. Wingate Hotel on October 17, 2017 [Minor 1 was age 15], and March 27-28, 2018 [Minor 1 was age 16]; and
f. Red Roof Inn Edgewood on June 14, 2018, July 2-3, 2018 [Minor 1 was age 16].

Through Grand Jury Subpoena service, your affiant learned Swavely checked into the following hotel locations:

a. Econolodge, Pocomoke City, Maryland, July 12-13, 2017, August 18-19, 2017, October 6-8, 2017, and December 29-31, 2017;

b. Econolodge, Princess Ann, Maryland on May 12-14, 2017, and February 16-18, 2018; and

c. Red Roof Inn, Edgewood, Maryland on June 15-16, 2017, and July 1-3, 2018.

15. Baltimore, Maryland is a location to which Swavely advised FPD he traveled with Minor 1 to visit the National Aquarium and go fishing. There are numerous pictures from the National Aquarium contained on Swavely's cellular telephone. Swavely's cellular telephone contains a picture of Minor 1 on board the 'Spirit of Baltimore,' a Baltimore Inner Harbor tour cruise in Baltimore, Maryland on July 14, 2017, a picture of the outside of a hotel taken on July 14, 2017, and an image of Minor 1 fishing on July 15, 2017. Minor 1 would have been age 15 on both of those dates. On both of those dates, Swavely's cellular telephone linked to a wifi connection at a Comfort Inn (your affiant has yet to learn of the exact location of this Comfort Inn, but suspects it is within the Baltimore, Maryland area due to the location of the photographs taken in Baltimore at that time.)

16. On January 10, 2020, Swavley was arrested by FPD on local charges relating to sexual acts with Minor 1. Swavely was arrested in his residence's outside basement room. During the arrest, body cameras worn by FPD showed one computer, an Acer laptop, on a work bench in the basement room. Later, Swavely's neighbor, Ray Nester, put a board across the basement door to keep it secured.

17. Swavely then sent a letter from prison to a friend, George Manwiller, and requested Manwiller go to the basement room and secure items, and unplug anything still running. On or about January 22 or 23, 2020, Manwiller, along with Nester and another friend of Swavely's, Brian Zimmerman, entered the basement and secured personal items and removed them from the basement. One of the items secured by Nester was a black computer bag containing Swavely's Acer laptop.

18. On January 30, 2020, your affiant obtained a search warrant from the Honorable Richard A. Lloret, United States Magistrate Judge, to search the outer rear basement of 121 South Chestnut Street, Fleetwood, Pennsylvania, 19522, Swavely's residence. The search warrant was executed on February 4, 2020. There were no computers on the premises. There were cords on a workbench suggesting that a computer had been there but had been removed.

19. On February 6, 2020, your affiant made contact with Nester to confirm he secured Swavely's basement by placing the board across the door, and to ask whether anyone entered the basement between the time Nester secured the basement and the FBI's search. Nester confirmed that he, Manwiller, and Zimmerman had entered the basement at Swavely's request, and had removed Swavely's work computer.

20. Nester believed the laptop he had secured in January 2020 belonged to Swavely's employer, Silfie's Trucking. To assist Swavely's elderly mother in returning the laptop case and laptop, Nester contacted Silfie's Trucking on February 7, 2020. Silfie's Trucking advised Nester that the laptop was not theirs and must belong to Swavely. Nester contacted your affiant to relinquish the computer to the FBI.

21. On February 7, 2020, your affiant took possession of the laptop case and its contents. Upon conducting an inventory of the laptop case, along with the Acer laptop, Serial Number 05205585825, your affiant also located a TLC/Tracphone cellular telephone, IMEI 015283000863287, and an 'Attache' 2 gigabyte thumb drive. Also in the laptop case was an Assateague Island National Seashore parking receipt dated April 1, 2017 (the Assateague Island National Seashore is approximately 20 miles from both Pocomoke City, Maryland and Princess Ann, Maryland).

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER/PHONE SYSTEMS

22. Searches and seizures of evidence from computer devices, cell phones, smart phones, and GPS's commonly require agents to download or copy information from the devices and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following:

a. Computer devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, cell phones, smart phones, GPS's, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take days or weeks, depending on the volume of data stored, and it would be generally difficult to accomplish this kind of data search on site; and

b. Searching computer and electronic systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

23. In addition, there is probable cause to believe that these computer and electronic devices contain evidence of violations of 18 U.S.C. § 2423 and should all be searched and seized as such.

SEARCH METHODOLOGY TO BE EMPLOYED

24. To search for electronic data contained in computer, phone, or electronic device hardware, computer, phone, or electronic device software, and/or memory storage devices, the examiners will make every effort to use computer forensic software to have a computer search the digital storage media. This may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

a. searching for image files to locate images of Minor 1, or any children, taken by or in the presence of Swavely;

b. surveying various file directories and the individual files they contain;

c. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set

forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

d. examination of all of the data contained in such computer hardware, computer software, and/or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;

e. scanning storage areas;

f. performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment B;

g. searching for malware in order to evaluate defenses, such as viruses; and/or

h. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

ABILITY TO RETRIEVE DELETED FILES

25. Computer files or remnants of such files on traditional or conventional mechanical computer hard drives can typically be recovered months or even years after they have been downloaded onto the hard drive, deleted or viewed via the Internet. Electronic files downloaded to the hard drive or storage device can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily available forensic tools. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files may reside in free space or slack space that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from these conventional types of hard drives depends less on when the file was downloaded or viewed than on the particular user's operating system, storage capacity, and computer habits.

26. Other than the conventional mechanical hard drives that are traditionally in computers, becoming more prevalent are flash memory based hard drives and devices. This

technology has been traditionally used for small thumb drives where files and data are stored electronically but has since evolved and is being used in computer hard drives known as "solid state hard drives" or SSD's, and also being used in cell phones and smart phones. These devices do not operate like mechanical hard drives when it comes to how files and data are stored and deleted. These devices can move data around on the drive to maximize storage space and longevity of the drive, compress data, and may use different deletion techniques for how a deleted file is handled and overwritten. Because of how these flash, memory-based drives function it may limit how much data, if any, can be recovered from these types of devices.

CONCLUSION

27. Based upon the information above I respectfully submit that there is probable cause to believe violations of 18 U.S.C. § 2423 have been committed, and that evidence, contraband, fruits and instrumentalities of those violations, further described in Attachment B, is located on: (a) an Acer laptop (Serial Number 05205585825); (b) a TCL/Tracphone (IMEI Number 015283000863287), and (c) an 'Attache' 2 gigabyte thumb drive, currently in the custody of FBI Philadelphia, further described in Attachment A. Therefore, I respectfully request that the attached warrant be issued.

28. I assert that public disclosure of the existence of this search warrant affidavit and all accompanying materials at this juncture could jeopardize the government's ongoing investigation in this case and therefore I request this affidavit and all accompanying material be sealed until further order of this Court.

Respectfully Submitted,

Benjamin M. Jacobs
Special Agent
Federal Bureau of Investigation

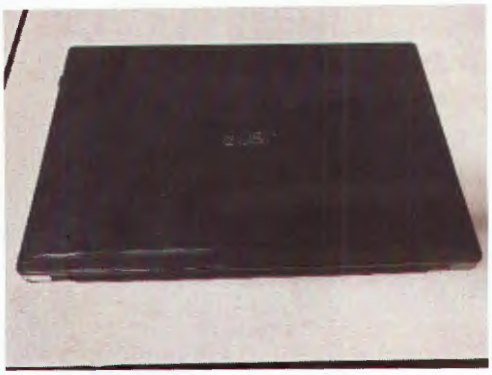
SWORN TO AND SUBSCRIBED
BEFORE ME THIS 19th DAY
OF FEBRUARY, 2020.

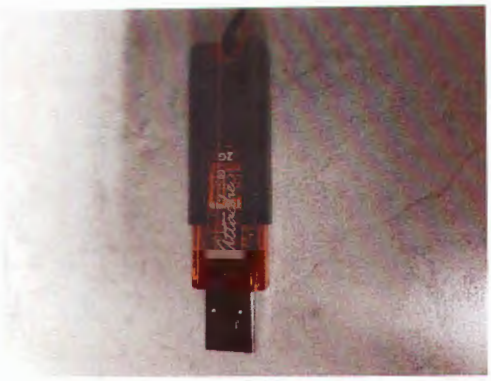
HONORABLE CAROL SANDRA MOORE WELLS
United States Magistrate Judge

ATTACHMENT A

Location to be Searched

1. Acer laptop, Serial Number 05205585825
2. TCL/Tracphone cellular telephone with a cracked screen, IMEI Number 015283000863287
3. 'Attache' 2 gigabyte thumb drive, orange/black in color





ATTACHMENT B

ITEMS TO BE SEARCHED FOR AND SEIZED

Evidence of violations of Title 18, United States Code, Section 2423, including the following:

1. All visual depictions of Minor 1, or any minor, on whatever medium (e.g. digital media, optical media, books, magazines, photographs, negatives, videotapes, CDs, DVDs, etc.), including those in opened or unopened emails. These include both originals and copies, and authorization is granted to remove videotapes without viewing them at the time and place of seizure, and to view them at a later time.

2. All documents, to include in electronic form, and stored communications, including contact information, text messages, call logs, voicemails, Internet searches, photographs, and any other electronic data or other memory features contained in the devices and SIM cards including correspondence, records, opened or unopened e mails, text messages, chat logs, and Internet history, pertaining to Swavely's out-of-state travel during the time period of 2012-2019, or relating to communication between Swavely and Minor 1.

3. All records, documents, invoices, notes and materials that pertain to the ownership or use of the computer equipment or electronic devices.

4. All records which evidence operation or ownership or use of computer or electronic equipment or devices, including, but not limited to, correspondence, sales receipts, bills, financial records, tax records, personal photographs, telephone records, notebooks, diaries, reference materials, or other personal items, and registration information for any software on the computer or device.

5. Documents and records regarding the ownership and/or possession of the searched premises.

6. All computer or electronic device passwords, keywords and other data security devices designed to restrict access to or hide computer software, documentation or data. Data security devices may consist of hardware, software, or other programming code. Any password or encryption key that may control access to a computer/phone operating system, individual computer/phone files, or other electronic data.

7. Evidence and contents of logs and files on a computer, electronic device, or storage device, such as those generated by the computer's operating system, which describes the history and use of the device, including but not limited to files indicating when files were written, were opened, were saved, or were deleted. Evidence tending to show the identity of the person using the computer or device at the time any of the items described in paragraph 1-3 were created, sent, received, or viewed. Also, any malware resident on the computer/phone or device.

8. The following may be seized and searched for all items listed above, and for any items specifically noted in the paragraphs below:

Computer hardware, meaning any and all computer equipment. Included within the definition of computer hardware are any electronic devices capable of data processing (such as central processing units, laptop or notebook or netbook or tablet computers, personal digital assistants, gaming consoles, and wireless communication devices to include cellular telephone devices capable of Internet access); peripheral input/output devices (such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media); related communications devices (such as modems, wireless routers, cables and connections, web cameras, microphones); storage media, defined below; and security devices, also defined below.

Computer software, meaning any and all data, information, instructions, programs, or program codes, stored in the form of electronic, magnetic, optical, or other media, which is capable of being interpreted by a computer or its related components. Computer software may also include data, data fragments, or control characters integral to the operation of computer software, such as operating systems software, applications software, utility programs, compilers, interpreters, communications software, and other programming used or intended to be used to communicate with computer components.

Computer related documentation, meaning any written, recorded, printed, or electronically stored material that explains or illustrates the configuration or use of any seized computer hardware, software, or related items.

Data security devices, meaning any devices, programs, or data whether themselves in the nature of hardware or software that can be used or are designed to be used to restrict access to, or to facilitate concealment of, any computer hardware, computer software, computer related documentation, or electronic data records. Such items include, but are not limited to, user names and passwords; data security hardware (such as encryption devices, chips, and circuit boards); data security software or information (such as test keys and encryption codes); and similar information that is required to access computer programs or date or to otherwise render programs or data into usable form.

All storage media capable of collecting, storing, maintaining, retrieving, concealing, transmitting, and backing up electronic data. Included within this paragraph is any information stored in the form of electronic, magnetic, optical, or other coding on computer media or on media capable of being read by a computer or computer related equipment, such as fixed hard disks, external hard disks, removable hard disks (including micro drives), floppy diskettes, compact disks (CDs), digital video disks (DVDs), tapes, optical storage devices, laser disks, thumb drives, ipods, digital cameras, memory cards (e.g. CF or SD cards), Xboxes, flash drives, or other memory storage devices. This also includes areas with digital storage capability on devices such as printers, scanners, wireless routers, etc.

The above seizure of computer and computer related hardware relates to such computer related items as being the instrumentalities of crime and also to allow for analysis/search for evidence of crime in an appropriate forensic setting. Upon a determination that such examination would be more appropriately made in a controlled environment, this storage media may be removed and examined at a laboratory location.